I CLAIM:

1. A communications device for secure communications in a highly dynamic environment between members of a predefined communications group that includes a plurality of group members, comprising:

an orthogonal code module for maintaining an orthogonal code table by reciprocally exchanging an orthogonal code with a communications device operated by each new member that joins the group, and deleting from the table the orthogonal code associated with the communications device of any group member that leaves the group;

an encryption module for encrypting a message to be sent to one or more of the group members using the orthogonal code associated with respective communications devices operated by the group members to which the message is to be sent; and

a decryption module for decrypting a message sent from a communications device operated by any of the other group members.

2. The communications device as claimed in claim 1 further comprising an orthogonal code generator module for generating the orthogonal codes.

3. The communications device as claimed in claim 1 further comprising a message amalgamating module for amalgamating a number of messages addressed to other group members into an amalgamated message.

4. The communications device as claimed in claim 2 wherein said orthogonal code module comprises an orthogonal generator for generating a set of orthogonal and pseudo random orthogonal codes that are of identical length.

5. The communications device as claimed in claim 1 wherein said orthogonal code table comprises a group member list, an encryption orthogonal code list, a decryption orthogonal code list and an unused orthogonal code list.

6. The communications device as claimed in claim 3 wherein said message amalgamating module comprises a plurality of adders that output an amalgamated message by adding together encrypted messages addressed to a plurality of group members encrypted using respective encryption orthogonal codes associated with communications devices operated by the group members to which the respective messages are addressed.

7. The communications device as claimed in claim 6 wherein said encryption module comprises an orthogonal code transformation function, a binary transformation module and an encryption function.

8. The communications device as claimed in claim 6 wherein said orthogonal code transformation function transforms an encryption orthogonal code to bipolar form in which each orthogonal code '1' is converted to '+1', and each orthogonal code '0' is converted to '-1'.

9. The communications device as claimed in claim 6 wherein said binary transformation module transforms the messages into a binary format.

10. The communications device as claimed in claim 9 wherein the encryption function accepts the message in binary format as input, examines each bit of the message and substitutes the bit with the encryption orthogonal code when the bit is "1" and a negative of said orthogonal code when the bit is "0".

11. The communications device as claimed in claim 10 wherein a plurality of encryption functions work in parallel so that a number of messages are encrypted concurrently.

12. The communications device as claimed in claim 6 wherein the plurality of adders comprise parallel adders and a combining adder for combining outputs of the plurality of parallel adders.

13. The communications device as claimed in claim 12 wherein the parallel adders add the encrypted messages bit by bit in parallel, and output the sum to the combining adder.

14. The communications device as claimed in claim 13 wherein the combining adder accepts the outputs of the parallel adders and adds the accepted outputs bit by bit to generate the amalgamated message.

15. The communications device as claimed in claim 1 wherein said decryption module comprises

a function for accessing to the orthogonal code table to obtain a decryption orthogonal code associated with the communications device operated by the group member who sent the message; and

a function for computing a normalized inner product of the decryption orthogonal code and the received message to decrypt the message.

16. The communications device as claimed in claim 1 wherein said orthogonal code module comprises a function for sending an orthogonal code to each new group member and a function for confirming receipt of an orthogonal code by the new group member.

17. The communications device as claimed in claim 16 wherein the function for sending orthogonal codes comprises means for encrypting respective orthogonal codes for a number of recipients, concatenating the encrypted orthogonal codes and broadcasting the concatenated orthogonal codes.

18. A method of providing secure communications in a highly dynamic environment between members of a predefined communications group that includes a plurality of group members, comprising:

maintaining an orthogonal code table for each group member by reciprocally exchanging an orthogonal code with each new member that joins the group, and deleting from the table the orthogonal code associated with any group member that leaves the group;

encrypting a message to be sent to one or more of the group members using the orthogonal code associated with respective group members to which the message is to be sent; and

decrypting a message sent from a communications device operated by any of the other group members.

19. The method as claimed in claim 18 wherein exchanging an orthogonal code with each new member that joins the group further comprises encrypting the orthogonal code prior to sending the orthogonal code to the new member.

20. The method as claimed in claim 19 wherein the encrypting comprises encrypting each orthogonal code using one of:

symmetric encryption if a sender of the orthogonal code has a pre-arranged shared symmetric key with the recipient, and otherwise using public key encryption with a public key of the recipient.

21. The method as claimed in claim 20 wherein said pre-arranged shared symmetric key is exchanged offline between the two parties before the secure group communication occurs.

22. The method as claimed in claim 20 wherein the public key is obtained from a directory service.

23. The method as claimed in claim 18 further comprising a step of confirming the exchange of orthogonal codes with each member, comprising:

collecting all orthogonal codes sent during a predetermined period of time;

encrypting acknowledgements for each member that sent an orthogonal code using the an encryption module, and broadcasting a resulting amalgamated encrypted acknowledgement message.

24. The method as claimed in claim 18 further comprising:

periodically generating a new set of orthogonal codes using an orthogonal code generating module;

assigning said new set of orthogonal codes to respective other group members;

encrypting and amalgamating the assigned orthogonal codes to form a new code message;

sending the new code message to the other group members; and

recording the update in related orthogonal code tables.

25. The method as claimed in claim 18 wherein when a member leaves the group, the method further comprises:

deleting the encryption code assigned to said leaving member;

deleting the decryption code assigned by said leaving member; and

deleting an identity of the leaving member from a group members list.

26. The method as claimed in claim 18 wherein when a new member joins the group, the method further comprises:

sending a join request to all group members with which the new member desires secure communications;

receiving a refusal acknowledgment from each group member that does not desire secure communications with the new member;

exchanging orthogonal codes with each group member that accepts communications with the new member; and

updating the orthogonal code table as the orthogonal codes are received from other group members.